UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/645,376	08/24/2000	Michael Scott Probasco	NC13977	3555

7590 10/31/2005

Nokia Inc
6000 Connection Drive 1-4-755
Irving, TX 75039

EXAMINER	
CALLAHAN, PAUL E	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 10/31/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/645,376	PROBASCO	
	Examiner	Art Unit	
	Paul Callahan	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 August 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 8-10-2005 has been entered.

2. Claims 1-18 were pending at the time of the previous Office Action. Claims 15-18 have been cancelled via the latest amendment. Therefore claims 1-14 are pending and have been examined.

Response to Arguments

3. Applicant's arguments with respect to claims 1-14 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al. US 5,870,474, Itkis, US 6,880,081, and Wallner et al.: Network Working Group, Request For Comments 2627, June 1999: "Key Management For Multicast, Issues And Architectures."

As for claims 1, 6, 8, and 11, Wasilewski teaches a method and means for carrying out the method for sending secure messages in a broadcast network (abstract) comprising the steps of: encrypting data with a key (col. 3 lines 43-67); hashing said key (col. 4 lines 1-25), combining said encrypted data and said key in a broadcast message capable of being decrypted by each of a plurality of receiving nodes (col. 3 lines 43-67), and transmitting said broadcast message to the plurality of receiving nodes (abstract). However Wasilewski does not teach wirelessly transmitting said messages. However Wallner et al do teach this feature in Section 2.0 Introduction. Wasilewski also fails to teach removing at least one node form the plurality of wireless nodes by transmitting a NULL key to the node to be removed such that the removed node is thereafter unable to decrypt a broadcast message encrypted with said key. However Itkis does teach this feature in col. 12 lines 35-67. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features of Wallner and Itkis into the system of Wasilewski. The motive to combine is found, for example, at col. 1 lines 13-45 where the problem of removal or "blacklisting" nodes is discussed.

As for claims 2 and 3, Wasilewski teaches a plurality of keys (col. 3 lines 43-67), and a combining step that comprises combining said encrypted data with each one of said plurality of different keys in a plurality of (categories of) broadcast messages (abstract, col. 4 lines 1-25), and transmitting one of the plurality of broadcast messages to a subset of said plurality of receiving nodes (abstract).

As for claims 4, 9, 10, and 13, Wasilewski teaches a method and means for carrying out the method for decrypting a message received over a broadcast network (abstract) comprising the steps of: receiving data comprising an encrypted message and a hashed key at a node in said broadcast network (abstract) where said node comprises means for storing data (fig. 1 items 90a – 90n "Customers STU's"); parsing said data to derive said encrypted message and said hashed key (col. 11 lines 24-30); comparing said received hashed key with a plurality of keys pre-stored in said means for storing data in said node and to select a key having a hash matching said received hashed key and decrypting said encrypted message with said matching key if a match is found (col. 11 lines 24-67).

As for claim 5, Wasilewski teaches requesting a key from a network entity if no prestored key has a hash that matches said received key (col. 11 lines 48-50).

As for claim 7, Wasilewski teaches all of the limitations of claim 5 upon which claim 7 is dependent but doesn't teach a network entity that distributes hashed keys as

per claim 7. Official Notice may be taken however that such a feature is old and well known in the art of cryptographic communications. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Wasilewski. It would have been desirable to do so as to increase the security of key distribution. Wasilewski discusses the advantage of making this combination at for example col. 4 lines 1-25 where the desirability of transmitting keys in hashed form is explained.

As for claim 12, Wasilewski teaches a tangible medium that is a hard disk or the like (fig. 11 item 196).

As for claim 14, Wasilewski teaches parsing, comparing, and decrypting steps that are carried out at each of a plurality of nodes (col. 11 lines 24-67)

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone

number for the organization where this application or proceeding is assigned is: (571) 273-8300.

10/25/2005

Paul Callahan

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER